B4 98P1764

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 195 18 544 C 1**

(51) Int. Cl.[6]:
H 04 L 9/00
G 06 F 12/14

(21) Aktenzeichen: 195 18 544.7-31
(22) Anmeldetag: 19. 5. 95
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 1. 8. 96

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Horn, Günther, Dr., 81541 München, DE; Kessler, Volker, Dr., 85256 Vierkirchen, DE; Müller, Klaus, 81539 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 52 22 140
US 52 14 700
US 51 53 919

DE-Broschüre: Telesec. Telekom, Produktentwicklung Telesec beim Fernmneldeamt Siegen, S.12-13 und Bild 16;
US-Z.: AZIZ, A., DIFFIE, W.: Privacy and Authentication for Wireless Local Area Networks. In: IEEE Personal Communications, 1994, S. 25-31;
US-Z.: BELLER, M.: Proposed Authentication and Key Agreement Protocol for Personal Communications, P&A JEM 1993, S. 1-11;
US-Z.: BELLER, M. et al.: Privacy and Authentication on a Portable Communication System. In: IEEE Journal on Selected Areas in Communications, Vol. 11, No. 6, 1993, S. 821-829;

(54) Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit und einer Netzcomputereinheit

(57) Die Erfindung betrifft ein Verfahren, mit dem ein Sitzungsschlüssel (K) zwischen einer Benutzercomputereinheit (U) und einer Netzcomputereinheit (N) vereinbart werden kann, ohne daß ein unbefugter Dritter nützliche Information bezüglich der Schlüssel oder der Identität der Benutzercomputereinheit (U) erhalten kann. Dies wird erreicht durch die Einbettung des Prinzips des El-Gamal Schlüsselaustauschs in das erfindungsgemäße Verfahren. Durch die Verwendung zweier Zufallszahlen (t, r) wird die Aktualität des Sitzungsschlüssels (K) gewährleistet. Der Sitzungsschlüssel (K) selbst wird niemals übertragen und kann somit nicht von einem unbefugten Dritten ermittelt werden.
Außerdem bietet das erfindungsgemäße Verfahren zusätzliche Sicherheitsmechanismen, wie z. B. die explizite Authentifikation der Netzcomputereinheit (N) durch die Benutzercomputereinheit (U) oder auch die Betätigung des Sitzungsschlüssels (K) von der Netzcomputereinheit (N) an die Benutzercomputereinheit (B).

DE 195 18 544 C 1

DE 195 18 544 C 1

Beschreibung

Informationstechnische Systeme unterliegen verschiedenen Bedrohungen. So kann z. B. übertragene Information von einem unbefugten Dritten abgehört und verändert werden. Eine weitere Bedrohung bei der Kommunikation zweier Kommunikationspartner liegt in der Vorspiegelung einer falschen Identität eines Kommunikationspartners.

Diesen und weiteren Bedrohungen wird durch verschiedene Sicherheitsmechanismen, die das informationstechnische System vor den Bedrohungen schützen sollen, begegnet. Ein zur Sicherung verwendet er Sicherheitsmechanismus ist die Verschlüsselung der übertragenen Daten. Damit die Daten in einer Kommunikationsbeziehung zwischen zwei Kommunikationspartnern verschlüsselt werden können, müssen vor der Übertragung der eigentlichen Daten erst Schritte durchgeführt werden, die die Verschlüsselung vorbereiten. Die Schritte können z. B. darin bestehen, daß sich die beiden Kommunikationspartner auf einen Verschlüsselungsalgorithmus einigen und daß ggf. die gemeinsamen geheimen Schlüssel vereinbart werden.

Besondere Bedeutung gewinnt der Sicherheitsmechanismus Verschlüsselung bei Mobilfunksystemen, da die übertragenen Daten in diesen Systemen von jedem Dritten ohne besonderen zusätzlichen Aufwand abgehört werden können.

Dies führt zu der Anforderung, eine Auswahl bekannter Sicherheitsmechanismen so zu treffen und diese Sicherheitsmechanismen geeignet zu kombinieren, sowie Kommunikationsprotokolle zu spezifizieren, daß durch sie die Sicherheit von informationstechnischen Systemen gewährleistet wird.

Es sind verschiedene asymmetrische Verfahren zum rechnergestützen Austausch kryptographischer Schlüssel bekannt. Asymmetrische Verfahren, die geeignet sind für Mobilfunksysteme, sind (A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) und (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11).

Das in (A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) beschriebene Verfahren bezieht sich ausdrücklich auf lokale Netzwerke und stellt höhere Rechenleistungsanforderungen an die Computereinheiten der Kommunikationspartner während des Schlüsselaustauschs. Außerdem wird in dem Verfahren mehr Übertragungskapazität benötigt als in dem erfindungsgemäßen Verfahren, da die Länge der Nachrichten größer ist als bei dem erfindungsgemäßen Verfahren.

Das in (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11) beschriebene Verfahren hat einige grundlegende Sicherheitsziele nicht realisiert. Die explizite Authentifikation des Netzes durch den Benutzer wird nicht erreicht. Außerdem wird ein vom Benutzer an das Netz übertragener Schlüssel vom Netz nicht an den Benutzer bestätigt. Auch eine Zusicherung der Frische (Aktualität) des Schlüssels für das Netz ist nicht vorgesehen. Ein weiterer Nachteil dieses Verfahrens besteht in der Beschränkung auf das Rabin-Verfahren bei der impliziten Authentifizierung des Schlüssels durch den Benutzer. Dies schränkt das Verfahren in einer flexibleren Anwendbarkeit ein. Außerdem ist kein Sicherheitsmechanismus vorgesehen, der die Nichtabstreitbarkeit von übertragenen Daten gewährleistet. Dies ist ein erheblicher Nachteil vor allem auch bei der Erstellung unanfechtbarer Gebührenabrechnungen für ein Mobilfunksystem. Auch die Beschränkung des Verfahrens auf den National Institute of Standards in Technology Signature Standard (NIST DSS) als verwendete Signaturfunktion schränkt das Verfahren in seiner allgemeinen Verwendbarkeit ein.

Aus der US-Patentschrift US 5 222 140 ist ein Verfahren bekannt, bei dem unter Verwendung sowohl eines öffentlichen als auch eines geheimen Schlüssels sowie unter Verwendung einer Zufallszahl ein Sitzungsschlüssel erzeugt wird. Dieser wird mit einem öffentlichen Schlüssel verknüpft.

Dieses Verfahren weist im Vergleich zu dem erfindungsgemäßen Verfahren weniger realisierte grundlegende Sicherheitsziele auf.

Weiterhin ist aus der Patentschrift US 5 153 919 ein Verfahren beschrieben, bei dem eine Benutzereinheit sich gegenüber einer Netzeinheit identifiziert. Anschließend findet unter Anwendung einer Hash-Funktion zwischen der Benutzereinheit und der Netzeinheit ein Authentifizierungsprozeß statt.

Weitere sichere Kommunikationsprotokolle, die aber wesentliche grundlegende Sicherheitsziele nicht realisieren, sind bekannt (M. Beller et al, Privacy and Authentication on a Portable Communication System, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 6, S. 821—829, 1993).

Das Problem der Erfindung liegt darin, ein Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel anzugeben, das die oben genannten Nachteile vermeidet.

Dieses Problem wird durch das Verfahren gemäß Patentanspruch 1 gelöst.

Die durch das erfindungsgemäße Verfahren erreichten Vorteile liegen vor allem in einer erheblichen Reduktion der Länge der übertragenen Nachrichten und in der Realisierung weiterer Sicherheitsziele.

Durch das erfindungsgemäße Verfahren werden folgende Sicherheitsziele realisiert:

- Gegenseitige explizite Authentifizierung von dem Benutzer und dem Netz, d. h. die gegenseitige Verifizierung der behaupteten Identität,
- Schlüsselvereinbarung zwischen dem Benutzer und dem Netz mit gegenseitiger impliziter Authentifizierung, d. h. daß durch das Verfahren erreicht wird, daß nach Abschluß der Prozedur ein gemeinsamer geheimer Sitzungsschlüssel zur Verfügung steht, von dem jede Partei weiß, daß nur das authentische Gegenüber sich ebenfalls im Besitz des geheimen Sitzungsschlüssels befinden kann,
- Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für den Benutzer,
- gegenseitige Bestätigung des Sitzungsschlüssels von dem Benutzer und dem Netz, d. h. die Bestätigung, daß das Gegenüber tatsächlich im Besitz des vereinbarten geheimen Sitzungsschlüssels ist,
- Senden eines Zertifikats für den öffentlichen Schlüssel des Netzes vom Netz an den Benutzer,
- Senden eines Zertifikats für den öffentlichen Schlüssel des Benutzers von der Zertifizierungsinstanz an das Netz,

— Zusicherung der Frische (Aktualität) der Zertifikate für den öffentlichen Schlüssel des Benutzers und für den öffentlichen Schlüssel des Netzes.

Durch die Weiterbildung gemäß Patentanspruch 2 wird das Sicherheitsziel der Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für das Netz realisiert.

Die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 3 ermöglicht die Verwendung von temporären Benutzeridentitäten.

Durch die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 4 wird das Sicherheitsziel der Benutzeranonymität realisiert, d. h. die Vertraulichkeit der Identität des Benutzers gegenüber Dritten.

Durch die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 6 wird zusätzlich das Sicherheitsziel der Nichtabstreitbarkeit von Daten realisiert, die vom Benutzer an das Netz gesendet werden.

Das erfindungsgemäße Verfahren ist außerdem sehr leicht an unterschiedliche Anforderungen anpaßbar, da es sich nicht auf bestimmte Algorithmen für Signaturbildung und Verschlüsselung beschränkt.

Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Die Zeichnungen stellen bevorzugte Ausführungsbeispiele der Erfindung dar, die im folgenden näher beschrieben werden.

Es zeigen

Fig. 1a, b ein Ablaufdiagramm, das das erfindungsgemäße Verfahren gemäß Patentanspruch 1 darstellt;

Fig. 2a, b ein Diagramm, das das erfindungsgemäße Verfahren mit zusätzlich realisierten Sicherheitszielen gemäß einiger abhängiger Patentansprüche beschreibt.

Anhand der **Fig.** 1a, b und 2a, b wird die Erfindung weiter erläutert.

In den **Fig.** 1a, b sind durch zwei Skizzen der Ablauf des erfindungsgemäßen Verfahrens dargestellt. Das erfindungsgemäße Verfahren betrifft den Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit U und einer Netzcomputereinheit N, wobei unter der Benutzercomputereinheit U eine Computereinheit eines Benutzers eines Mobilfunknetzes zu verstehen ist und unter einer Netzcomputereinheit N eine Computereinheit des Netzbetreibers eines Mobilfunksystems zu verstehen ist.

Die Erfindung beschränkt sich jedoch nicht auf ein Mobilfunksystem und somit auch nicht auf einen Benutzer eines Mobilfunksystems und das Netz, sondern kann in allen Bereichen angewendet werden, in denen ein kryptographischer Schlüsselaustausch zwischen zwei Kommunikationspartnern benötigt wird. Dies kann z. B. in einer Kommunikationsbeziehung zwischen zwei Rechnern, die Daten in verschlüsselter Form austauschen wollen, der Fall sein. Ohne Beschränkung der Allgemeingültigkeit wird im folgenden also ein erster Kommunikationspartner als Benutzercomputereinheit U und ein zweiter Kommunikationspartner als Netzcomputereinheit N bezeichnet.

Für das erfindungsgemäße Verfahren gemäß Anspruch 1 wird vorausgesetzt, daß in der Benutzercomputereinheit U kein vertrauenswürdiger öffentlicher Netzschlüssel g^s der Netzcomputereinheit N verfügbar ist. In der Benutzercomputereinheit U ist ein vertrauenswürdiger öffentlicher Zertifizierungsschlüssel g^u der Zertifizierungscomputereinheit CA verfügbar, wobei g ein erzeugendes Element einer endlichen Gruppe ist. Dies bedeutet, daß die Benutzercomputereinheit U sich den vertrauenswürdigen öffentlichen Netzschlüssel g^s in Form eines Netzzertifikats CertN von einer Zertifizierungscomputereinheit CA "besorgen" muß. Ebenso braucht die Netzcomputereinheit N den vertrauenswürdigen öffentlichen Benutzerschüssel öu in Form eines Benutzerzertifikats CertU von der Zertifizierungscomputereinheit CA.

In der Benutzercomputereinheit U wird eine erste Zufallszahl t generiert. Aus der ersten Zufallszahl t wird mit Hilfe des erzeugenden Elements g einer endlichen Gruppe in der Benutzercomputereinheit U ein erster Wert g^t gebildet.

Asymmetrische Verfahren beruhen im wesentlichen auf zwei Problemen der Komplexitätstheorie, dem Problem zusammengesetzte Zahlen effizient zu faktorisieren, und dem diskreten Logarithmusproblem (DLP). Das DLP besteht darin, daß in geeigneten Rechenstrukturen zwar Exponentiationen effizient durchgeführt werden können, daß jedoch für die Umkehrung dieser Operation, das Logarithmieren, keine effizienten Algorithmen bekannt sind.

Solche Rechenstrukturen sind z. B. unter den oben bezeichneten endlichen Gruppen zu verstehen. Diese sind z. B. die multiplikative Gruppe eines endlichen Körpers (z. B. Multiplizieren Modulo p, wobei p eine große Primzahl ist), oder auch sogenannte "elliptische Kurven". Elliptische Kurven sind vor allem deshalb interessant, weil sie bei gleichem Sicherheitsniveau wesentliche kürzere Sicherheitsparameter erlauben. Dies betrifft die Länge der öffentlichen Schlüssel, die Länge der Zertifikate, die Länge der bei der Sitzungsschlüsselvereinbarung auszutauschenden Nachrichten sowie die Länge von digitalen Signaturen, die jeweils im weiteren beschrieben werden. Der Grund dafür ist, daß die für elliptische Kurven bekannten Logarithmierverfahren wesentlich weniger effizient sind als die für endliche Körper.

Eine große Primzahl in diesem Zusammenhang bedeutet, daß die Größe der Primzahl so gewählt werden muß, daß die Logarithmierung so aufwendig ist, daß sie nicht in vertretbarer Zeit durchgeführt werden kann. Vertretbar bedeutet in diesem Zusammenhang einen Zeitraum entsprechend der Sicherheitspolitik von mehreren Jahren bis Jahrzehnten und länger.

Nach der Berechnung des ersten Werts g^t wird eine erste Nachricht M1 codiert, die mindestens den ersten Wert g^t, eine Identitätsgröße |MU| der Benutzercomputereinheit U und eine Identitätsgröße id_{CA} einer Zertifizierungscomputereinheit CA, die ein Netzzertifikat CertN liefert, das von der Benutzercomputereinheit U verifiziert werden kann, aufweist. Dies ist nötig, wenn mehrere Zertifizierungsinstanzen mit unterschiedlichen geheimen Zertifizierungsschlüsseln vorgesehen werden. Wenn das Sicherheitsziel der Benutzeranonymität realisiert werden soll, wird in der Benutzercomputereinheit vor Bildung der ersten Nachricht M1 ein Zwischenschlüssel L gebildet. Dies geschieht durch Potenzierung des öffentlichen Zertifizierungsschlüssels g^u mit der ersten Zufallszahl t. Im weiteren wird in diesem Fall die Identitätsgröße |MU| der Benutzercomputereinheit U mit dem Zwischenschlüssel L unter Anwendung einer Verschlüsselungsfunktion Enc verschlüsselt und das Ergebnis stellt einen vierten verschlüsselten Term VT4 dar. Der vierte verschlüsselte Term VT4 wird anstatt der Identitätsgröße |MU| der Benutzercomputereinheit U in die erste Nachricht M1 integriert. Die erste Nachricht M1 wird von der Benutzercomputereinheit U an

die Netzcomputereinheit N übertragen.

In der Netzcomputereinheit N wird die erste Nachricht M1 decodiert. Die erste Nachricht M1 kann auch über einen unsicheren Kanal, also auch übt eine Luftschnittstelle, unverschlüsselt übertragen werden, da die Logarithmierung des ersten Wertes g^t nicht in vertretbarer Zeit durchgeführt werden kann.

In der Netzcomputereinheit N wird die erste Nachricht M1 decodiert, und eine vierte Nachricht M4 gebildet, die eine Verkettung des der Netzcomputereinheit N bekannten öffentlichen Netzschlüssels g^s, dem ersten Wert g^t und der Identitätsgröße |MU| der Benutzercomputereinheit U, sowie einem ersten signierten Term aufweist. Der erste signierte Term wird gebildet durch Anwendung einer zweiten Signaturfunktion Sig_N auf einen ersten Signatureingangsterm. Der erste Signatureingangsterm weist mindestens ein Ergebnis einer dritten Hash-Funktion h3 auf, die auf mindestens eine Verkettung des öffentlichen Netzschlüssels g^s, des ersten Werts g^t und der Identitätsgröße |MU| der Benutzercomputereinheit U angewendet wird. In dem Fall, daß das Sicherheitsziel der Benutzeranonymität realisiert werden soll, wird in der vierten Nachricht M4 anstatt der Identitätsgröße |MU| der Benutzercomputereinheit U der vierte verschlüsselte Term VT4 codiert. In diesem Fall weist auch die Verkettung, auf die die dritte Hash-Funktion h3 angewendet wird, anstatt der Identitätsgröße |MU| der Benutzercomputereinheit U den vierten verschlüsselten Term VT4 auf.

Die zweite Signaturfunktion Sig_N kann, muß aber nicht gleich sein der ersten Signaturfunktion Sig_U.

Die vierte Nachricht M4 wird in der Netzcomputereinheit N codiert und anschließend an die Zertifizierungscomputereinheit CA übertragen.

In der Zertifizierungscomputereinheit CA wird die vierte Nachricht M4 decodiert und mit dem öffentlichen Schlüssel g^s, der der Zertifizierungscomputereinheit CA bekannt ist, verifiziert. Damit wird die Netzcomputereinheit N als Sender der vierten Nachricht M4 authentifiziert.

Anschließend wird, falls die Benutzeranonymität gewährleistet wird, also der vierte verschlüsselte Term VT4 in der vierten Nachricht M4 mitgesendet wurde, in der Zertifizierungscomputereinheit CA der Zwischenschlüssel L berechnet, indem der erste Wert g^t mit einem geheimen Zertifizierungsschlüssel u der Zertifizierungscomputereinheit CA potenziert wird.

Mit dem Zwischenschlüssel L wird unter Verwendung der Verschlüsselungsfunktion Enc der vierte verschlüsselte Term VT4 entschlüsselt, womit in der Zertifizierungscomputereinheit CA die Identitätsgröße |MU| der Benutzercomputereinheit U bekannt ist.

In der Zertifizierungscomputereinheit CA wird dann das Benutzerzertifikat CertU ermittelt. Das Benutzerzertifikat CertU kann z. B. aus einer der Zertifizierungscomputereinheit CA eigenen Datenbank ermittelt werden, die alle Zertifikate der Computereinheiten enthält, für die die Zertifizierungscomputereinheit CA Zertifikate erstellt.

Um die Gültigkeit des Netzzertifikats CertN und des Benutzerzertifikats CertU zu überprüfen, wird eine Identitätsangabe id_N und der in der vierten Nachricht mitgesendete öffentliche Netzschlüssel g^s, die Identitätsgröße |MU| der Benutzercomputereinheit U sowie das ermittelte Benutzerzertifikat CertU mit einer Revokationsliste verglichen, in der ungültige Zertifikate, Schlüssel oder Identitätsgrößen aufgeführt sind.

Anschließend wird aus mindestens einer Verkettung des ersten Werts g^t, des öffentlichen Netzschlüssels g^s und der Identitätsangabe id_N der Netzcomputereinheit N ein dritter Term gebildet.

Der dritte Term wird mit Hilfe einer vierten Hash-Funktion h4 "gehasht" und das Ergebnis der Hash-Funktion h4 wird unter Verwendung einer dritten Signaturfunktion Sig_{CA} signiert. Ein Netzzertifikat CertN wird nun in der Zertifizierungscomputereinheit CA gebildet, wobei das Netzzertifikat CertN mindestens den dritten Term und den signierten Hash-Wert des dritten Terms aufweist.

Weiterhin wird in der Zertifizierungscomputereinheit CA ein Zeitstempel TS kreiert.

In der Zertifizierungscomputereinheit CA wird außerdem ein fünfter Term gebildet, der mindestens eine Verkettung des Zeitstempels TS, der Identitätsangabe id_N der Netzcomputereinheit N und des Benutzerzertifikats CertU aufweist.

Ein zweiter signierter Term wird gebildet durch Anwendung der dritten Signaturfunktion Sig_{CA} auf einen zweiten Signatureingangsterm und den geheimen Zertifizierungsschlüssel u. Der zweite Signatureingangsterm weist mindestens ein Ergebnis der vierten Hash-Funktion h4 auf, die auf mindestens den fünften Term angewendet wird.

Anschließend wird ein sechster Term gebildet, der mindestens den fünften Term und den signierten Hash-Wert des fünften Terms aufweist.

Eine in der Zertifizierungscomputereinheit CA gebildete fünfte Nachricht M5 weist mindestens eine Verkettung aus dem Netzzertifikat CertN und dem sechsten Term auf.

Die fünfte Nachricht M5 wird in der Zertifizierungscomputereinheit CA codiert und an die Netzcomputereinheit N übertragen. Nachdem die fünfte Nachricht in der Netzcomputereinheit N decodiert ist, wird das Netzzertifikat CertN und der zweite signierte Term verifiziert.

In der Netzcomputereinheit N wird nun ein vierter Term gebildet, der mindestens eine Verkettung des öffentlichen Netzschlüssels g^s und des signierten Hash-Werts des dritten Terms aufweist.

In der Netzcomputereinheit N wird mit Hilfe einer ersten Hash-Funktion h1 ein Sitzungsschlüssel K gebildet. Als eine erste Eingangsgröße der ersten Hash-Funktion h1 wird eine Konkatenation eines ersten Terms mit der zweiten Zufallszahl r verwendet. Der erste Term wird gebildet, indem der erste Wert g^t potenziert wird mit einem geheimen Netzschlüssel s. Unter einer Hash-Funktion ist in diesem Zusammenhang eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfolge fester Länge zugeordnet. Des weiteren wird für die Hash-Funktion in diesem Zusammenhang Kollisionsfreiheit gefordert, d. h. es darf nicht möglich sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben. Die zweite Zufallszahl r findet Verwendung, wie in den Fig. 2a, b beschrieben, wenn das zusätzliche Sicherheitsziel der Zusicherung der Frische (Aktualität) des Sitzungsschlüssels K für die Netzcomputereinheit N realisiert werden soll. Ist dieses Sicherheitsziel nicht benötigt, wird die zweite Zufallszahl r nicht in dem erfindungsgemäßen Verfahren verwendet.

Nun wird in der Netzcomputereinheit N eine Antwort A gebildet. Zur Bildung der Antwort A sind ver-

schiedene Varianten vorgesehen. So ist es z. B. möglich, daß mit dem Sitzungsschlüssel K unter Verwendung einer Verschlüsselungsfunktion Enc eine Konstante const verschlüsselt wird. Die Konstante const ist sowohl der Benutzercomputereinheit U als auch der Netzcomputereinheit N bekannt. Auch die Verschlüsselungsfunktion Enc ist sowohl der Netzcomputereinheit N als auch der Benutzercomputereinheit U als die in dem erfindungsgemäßen Verfahren zu verwendende Verschlüsselungsfunktion bekannt.

Eine weitere Möglichkeit, die Antwort A zu bilden liegt z. B. darin, daß der Sitzungsschlüssel K als Eingangsgröße für eine dritte Hash-Funktion h3 verwendet wird und der "gehashte" Wert des Sitzungsschlüssels K als Antwort A verwendet wird. Weitere Möglichkeiten, die Antwort A zu bilden, die zur Überprüfung des Sitzungsschlüssels K in der Benutzercomputereinheit U verwendet wird, sind dem Fachmann geläufig und können als Varianten zu den beschriebenen Vorgehensweisen verwendet werden.

Eine Aneinanderreihung der zweiten Zufallszahl r, des vierten Terms der Antwort A, sowie ein optionales erstes Datenfeld dat1 bilden eine zweite Nachricht M2. Die zweite Zufallszahl r und das optionale erste Datenfeld dat1 sind nur in der zweiten Nachricht M3 enthalten, wenn diese in dem erfindungsgemäßen Verfahren vorgesehen werden.

Die zweite Nachricht M2 wird in der Netzcomputereinheit N codiert und zu der Benutzercomputereinheit U übertragen.

In der Benutzercomputereinheit U wird die zweite Nachricht M2 decodiert, so daß die Benutzercomputereinheit U eventuell die zweite Zufallszahl r, die Antwort A sowie eventuell das optionale erste Datenfeld dat1 zur Verfügung hat. Die Länge des optionalen ersten Datenfeldes dat1 kann beliebig groß sein, d. h. es ist auch möglich, daß das optionale erste Datenfeld dat1 nicht vorhanden ist.

In der Benutzercomputereinheit U wird nun ebenfalls der Sitzungsschlüssel K gebildet, mit Hilfe der ersten Hash-Funktion h1, die sowohl der Netzcomputereinheit N als auch der Benutzercomputereinheit U bekannt ist. Eine zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der Benutzercomputereinheit U weist mindestens einen zweiten Term auf. Der zweite Term wird gebildet aus einer Exponentation eines öffentlichen Netzschlüssels g^s mit der ersten Zufallszahl t. Wenn die zweite Zufallszahl r in dem erfindungsgemäßen Verfahren vorgesehen wird, so weist die zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der Benutzercomputereinheit U zusätzlich die zweite Zufallszahl r auf.

Durch die Verwendung der ersten Zufallszahl t und der zweiten Zufallszahl r bei der Generierung des Sitzungsschlüssels K wird die Aktualität des Sitzungsschlüssels K gewährleistet, da jeweils die erste Zufallszahl t als auch die zweite Zufallszahl r nur für jeweils einen Sitzungsschlüssel K verwendet werden.

Somit wird eine Wiedereinspielung eines älteren Schlüssels als Sitzungsschlüssel K verhindert. Wenn aber für jeden neuen Sitzungsschlüssel K andere Zufallszahlen verwendet werden, so ist die Wahrscheinlichkeit, daß der verwendete Sitzungsschlüssel K von einem unbefugten Dritten schon herausgefunden wurde, wesentlich geringer. Damit ist die Gefahr, daß der Teil einer Nachricht, der mit dem Sitzungsschlüssel K verschlüsselt ist, von einem unbefugten Dritten entschlüsselt werden kann, erheblich reduziert.

Nachdem in der Benutzercomputereinheit U der Sitzungsschlüssel K gebildet wurde, wird anhand der empfangenen Antwort A überprüft, ob der in der Benutzercomputereinheit U gebildete Sitzungsschlüssel K mit dem Sitzungsschlüssel K, der in der Netzcomputereinheit N gebildet wurde, übereinstimmt.

Abhängig von den im vorigen beschriebenen Varianten zur Bildung der Antwort A sind verschiedene Möglichkeiten vorgesehen, den Sitzungsschlüssel K anhand der Antwort A zu überprüfen.

Eine Möglichkeit besteht z. B. darin, daß, wenn die Antwort A in der Netzcomputereinheit N durch Verschlüsselung der Konstante const mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc gebildet wurde, die Antwort A entschlüsselt wird, und somit die Benutzercomputereinheit U eine entschlüsselte Konstante const' erhält, die mit der bekannten Konstante const verglichen wird.

Die Überprüfung des Sitzungsschlüssels K anhand der Antwort A kann auch durchgeführt werden, indem die der Benutzercomputereinheit U bekannte Konstante const mit dem in der Benutzercomputereinheit U gebildeten Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird und das Ergebnis mit der Antwort A auf Übereinstimmung geprüft wird. Diese Vorgehensweise wird z. B. auch verwendet, wenn die Antwort A in der Netzcomputereinheit N gebildet wird, indem auf den Sitzungsschlüssel K die dritte Hash-Funktion h3 angewendet wird. In diesem Fall wird in der Benutzercomputereinheit U der in der Benutzercomputereinheit U gebildete Sitzungsschlüssel K als Eingangsgröße der dritten Hash-Funktion h3 verwendet. Der "gehashte" Wert des in der Benutzercomputereinheit U gebildeten Sitzungsschlüssel K wird dann mit der Antwort A auf Übereinstimmung geprüft. Damit wird das Ziel der Schlüsselbestätigung des Sitzungsschlüssels K erreicht.

Dadurch, daß bei der Berechnung des Sitzungsschlüssels K in der Netzcomputereinheit N der geheime Netzschlüssel s und bei der Berechnung des Sitzungsschlüssels K in der Benutzercomputereinheit U der öffentliche Netzschlüssel g^s verwendet werden, wird die Netzcomputereinheit N durch die Benutzercomputereinheit U authentifiziert. Dies wird erreicht, vorausgesetzt daß für die Benutzercomputereinheit U bekannt ist, daß der öffentliche Netzschlüssel g^s tatsächlich zur Netzcomputereinheit N gehört.

Im Anschluß an die Bestätigung des Sitzungsschlüssels K durch Überprüfung der Antwort A wird ein Signaturterm berechnet. Hierzu wird mit Hilfe einer zweiten Hash-Funktion h2 eine vierte Eingangsgröße gebildet. Die zweite Hash-Funktion h2 kann, muß aber nicht dieselbe Hash-Funktion sein wie die erste Hash-Funktion hl. Als eine dritte Eingangsgröße für die zweite Hash-Funktion h2 wird ein Term verwendet, der mindestens den Sitzungsschlüssel K enthält. Weiterhin kann die dritte Eingangsgröße das optionale erste Datenfeld dat1 oder auch ein optionales zweites Datenfeld dat2 enthalten, wenn deren Verwendung in dem erfindungsgemäßen Verfahren vorgesehen wird.

Es kann später nicht abgestritten werden, daß die Daten, die im ersten optionale Datenfeld dat1 und im zweiten optionalen Datenfeld dat2 enthalten sind, von der Benutzercomputereinheit U gesendet werden.

Die in dem ersten optionalen Datenfeld dat1 und in dem zweiten optionalen Datenfeld dat2 enthaltenen Daten können z. B. Telefonnummern, die aktuelle Zeit oder

ähnliche hierfür geeignete Parameter sein. Diese Information kann als Werkzeug für eine unanfechtbare Gebührenabrechnung verwendet werden.

Unter Verwendung einer ersten Signaturfunktion Sig_U wird der Signaturterm aus mindestens der vierten Eingangsgröße gebildet. Um einen höheren Sicherheitsgrad zu erzielen, kann der Signaturterm verschlüsselt werden. Der Signaturterm wird in diesem Fall mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt und bildet den ersten verschlüsselten Term VT1.

Bei Verwendung eines optionalen zweiten Datenfeldes dat2 wird in der Benutzercomputereinheit U ein dritter verschlüsselter Term VT3 berechnet, indem das optionale zweite Datenfeld dat2 mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird. Das optionale zweite Datenfeld dat2 kann auch unverschlüsselt, also im Klartext übertragen werden.

In der Benutzercomputereinheit U wird eine dritte Nachricht M3 gebildet und codiert, die mindestens aus dem ersten verschlüsselten Term VT1, und, wenn das optionale zweite Datenfeld dat2 verwendet wird, dem dritten verschlüsselten Term VT3 oder dem optionalen zweiten Datenfeld dat2 im Klartext besteht. Die dritte Nachricht M3 wird von der Benutzercomputereinheit U zu der Netzcomputereinheit N übertragen.

Zusätzlich wird die Authentifikation der Benutzercomputereinheit U gegenüber der Netzcomputereinheit N durch den Signaturterm in der dritten Nachricht M3 gewährleistet, durch deren Verwendung auch garantiert wird, daß die dritte Nachricht M3 tatsächlich aktuell von der Benutzercomputereinheit U gesendet wurde.

In der Netzcomputereinheit N wird die dritte Nachricht M3 decodiert und anschließend wird der erste verschlüsselte Term VT1 sowie eventuell der dritte verschlüsselte Term VT3 entschlüsselt. Anhand des Benuterzertifikats CertU, das der Netzcomputereinheit N zur Verfügung steht, wird der Signaturterm verifiziert.

Wenn die Verwendung des optionalen zweiten Datenfelds dat2 vorgesehen wird, weist die dritte Nachricht M3 zusätzlich mindestens den dritten verschlüsselten Term VT3 auf oder das optionale zweite Datenfeld dat2 in Klartext, wenn das optionale zweite Datenfeld dat2 in Klartext übertragen werden soll.

Wenn die dritte Nachricht M3 den ersten verschlüsselten Term VT1, den zweiten verschlüsselten Term VT2 oder den dritten verschlüsselten Term VT3 aufweist, werden diese in der Netzcomputereinheit N entschlüsselt. Dies geschieht für den eventuell vorhandenen ersten verschlüsselten Term VT1 vor der Verifikation des Signaturterms.

Wenn für das erfindungsgemäße Verfahren temporäre Benutzeridentitäten vorgesehen werden, so wird das im vorigen beschriebene Verfahren um einige Verfahrensschritte erweitert.

In der Netzcomputereinheit N wird für die Benutzercomputereinheit U eine neue temporäre Identitätsgröße TMUIN gebildet, die der Benutzercomputereinheit U im weiteren zugewiesen wird. Dies kann z. B. durch Generierung einer Zufallszahl oder durch Tabellen, in denen mögliche Identitätsgrößen abgespeichert sind, durchgeführt werden. Aus der neuen temporären Identitätsgröße TMUIN der Benutzercomputereinheit U wird in der Netzcomputereinheit N ein vierter verschlüsselter Term VT4 gebildet, indem die neue temporäre Identitätsgröße TMUIN der Benutzercomputereinheit U mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird.

In diesem Fall weist die zweite Nachricht M2 zusätzlich mindestens den vierten verschlüsselten Term VT4 auf. Der vierte verschlüsselte Term VT4 wird dann in der Benutzercomputereinheit U entschlüsselt. Nun ist die neue temporäre Identitätsgröße TMUIN der Benutzercomputereinheit U in der Benutzercomputereinheit U verfügbar.

Damit der Netzcomputereinheit N auch gewährleistet wird, daß die Benutzercomputereinheit U die neue temporäre Identitätsgröße TMUIN korrekt empfangen hat, weist die dritte Eingangsgröße für die erste Hash-Funktion h1 oder für die zweite Hash-Funktion h2 zusätzlich mindestens die neue temporäre Identitätsgröße TMUIN der Benutzercomputereinheit U auf.

Die in dem erfindungsgemäßen Verfahren verwendeten Hash-Funktionen, die erste Hash-Funktion h1, die zweite Hash-Funktion h2 und die dritte Hash-Funktion h3 und die vierte Hash-Funktion h4 können durch die gleiche, aber auch durch verschiedene Hash-Funktionen realisiert werden.

Patentansprüche

1. Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit (U) und einer Netzcomputereinheit (N),

— bei dem aus einer ersten Zufallszahl (t) mit Hilfe eines erzeugenden Elements (g) einer endlichen Gruppe in der Benutzercomputereinheit (U) ein erster Wert (g^t) gebildet wird,

— bei dem eine erste Nachricht (M1) von der Benutzercomputereinheit (U) an die Netzcomputereinheit (N) übertragen wird, wobei die erste Nachricht (M1) mindestens den ersten Wert (g^T), eine Identitätsgröße (|MU|) der Benutzercomputereinheit (U) und eine Identitätsangabe (id_{CA}) einer Zertifizierungscomputereinheit (CA), die der Benutzercomputereinheit (U) ein Netzzertifikat (CertN) liefert, das von der Benutzercomputereinheit (U) verifiziert werden kann,

— bei dem eine vierte Nachricht (M4) von der Netzcomputereinheit (N) an die Zertifizierungscomputereinheit (CA) übertragen wird, wobei die vierte Nachricht (M4) mindestens einen öffentlichen Netzschlüssel (g^s), den ersten Wert (g^t), die Identitätsgröße (|MU|) der Benutzercomputereinheit (U) als Eingangsgröße aufweist und wobei eine Ausgangsgröße der dritten Hash-Funktion (h3) unter Verwendung einer zweiten Signaturfunktion (Sig_N) signiert wird,

— bei dem in der Zertifizierungscomputereinheit (CA) der erste signierte Term verifiziert wird,

— bei dem in der Zertifizierungscomputereinheit (CA) ein dritter Term gebildet wird, der mindestens den ersten Wert (g^t), den öffentlichen Netzschlüssel (g^s) und eine Identitätsangabe (id_N) der Netzcomputereinheit (N) aufweist,

— bei dem in der Zertifizierungscomputereinheit (CA) unter Verwendung einer vierten Hash-Funktion (h4) ein Hash-Wert über den

dritten Term gebildet wird,

— bei dem in der Zertifizierungscomputereinheit (CA) der Hash-Wert über den dritten Term unter Verwendung einer dritten Signaturfunktion (Sig_{CA}) mit einem geheimen Zertifizierungsschlüssel (U) signiert wird,

— bei dem in der Zertifizierungscomputereinheit (CA) ein Netzzertifikat (CertN) gebildet wird, das mindestens den dritten Term und den signierten Hash-Wert des dritten Terms aufweist,

— bei dem in der Zertifizierungscomputereinheit (CA) auf einen fünften Term der mindestens einen Zeitstempel (TS), die Identitätsangabe (id_N) der Netzcomputereinheit (N) und ein Benutzerzertifikat (CertU) aufweist, eine vierte Hash-Funktion (h4) angewendet wird,

— bei dem der Hash-Wert des fünften Terms durch Verwendung der dritten Signaturfunktion (Sig_{CA}) mit dem geheimen Zertifizierungsschlüssel (cs) signiert und das Ergebnis den zweiten signierten Term darstellt,

— bei dem eine fünfte Nachricht (M5), die mindestens das Netzzertifikat (CertN), den fünften Term und den zweiten signierten Term aufweist, von der Zertifizierungscomputereinheit (CA) zu der Netzcomputereinheit (N) übertragen wird,

— bei dem in der Netzcomputereinheit (N) das Netzzertifikat (CertN) und der zweite signierte Term verifiziert werden,

— bei dem in der Netzcomputereinheit (N) ein vierter Term, der mindestens den öffentlichen Netzschlüssel (g^s) und den signierten Hash-Wert des dritten Terms aufweist, gebildet wird,

— bei dem in der Netzcomputereinheit (N) ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h1) gebildet wird, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit dem geheimen Netzschlüssel (s),

— bei dem in der Netzcomputereinheit (N) eine Antwort (A) gebildet wird,

— bei dem eine zweite Nachricht (M2) von der Netzcomputereinheit (N) an die Benutzercomputereinheit (U) übertragen wird, wobei die zweite Nachricht (M2) mindestens die Antwort (A) und den vierten Term aufweist,

— bei dem in der Benutzercomputereinheit (U) das Netzzertifikat (CertN) verifiziert wird,

— bei dem in der Benutzercomputereinheit (U) der Sitzungsschlüssel (K) gebildet wird mit Hilfe der ersten Hash-Funktion (h1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation des öffentlichen Netzschlüssels (g^s) mit der ersten Zufallszahl (t),

— bei dem in der Benutzercomputereinheit (U) der Sitzungsschlüssel (K) anhand der Antwort (A) überprüft wird,

— bei dem in der Benutzercomputereinheit (U) mit Hilfe einer zweiten Hash-Funktion (h2) oder der ersten Hash-Funktion (h1) eine vierte Eingangsgröße gebildet wird, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße mindestens den Sitzungsschlüssel (K) aufweist,

— bei dem in der Benutzercomputereinheit (U) ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet wird unter Anwendung einer ersten Signaturfunktion (Sig_U),

— bei dem eine dritte Nachricht (M3) von der Benutzercomputereinheit (U) an die Netzcomputereinheit (N) übertragen wird, wobei die dritte Nachricht (M3) mindestens den Signaturterm aufweist,

— bei dem in der Netzcomputereinheit (N) der Signaturterm verifiziert wird.

2. Verfahren nach Anspruch 1,

— bei dem in der Netzcomputereinheit (N) die erste Eingangsgröße der ersten Hash-Funktion (h1) zusätzlich mindestens eine zweite Zufallszahl (r) aufweist,

— bei dem die zweite Nachricht (M2) zusätzlich die zweite Zufallszahl (r) aufweist, und

— bei dem in der Benutzercomputereinheit (U) die zweite Eingangsgröße der ersten Hash-Funktion (h1) zusätzlich mindestens die zweite Zufallszahl (r) aufweist.

3. Verfahren nach Anspruch 1 oder 2,

— bei dem in der Netzcomputereinheit (N), nachdem die erste Nachricht (M1) empfangen wurde und bevor die zweite Nachricht (M2) gebildet wird, für die Benutzercomputereinheit (U) eine neue temporäre Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) gebildet wird,

— bei dem in der Netzcomputereinheit (N) aus der neuen temporären Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) ein vierter verschlüsselter Term (VT4) gebildet wird, indem die neue temporäre Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) mit dem Sitzungsschlüssel (K) unter Verwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die zweite Nachricht (M2) zusätzlich mindestens den vierten verschlüsselten Term (VT4) aufweist,

— bei dem in der Benutzercomputereinheit (U), nachdem die zweite Nachricht (M2) empfangen wurde und bevor die vierte Eingangsgröße gebildet wird, der vierte verschlüsselte Term (VT4) entschlüsselt wird, und

— bei dem die dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße zusätzlich mindestens die neue temporäre Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) aufweist.

4. Verfahren nach einem der Ansprüche 1 bis 3,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der ersten Nachricht (M1) ein Zwischenschlüssel (L) gebildet wird, indem ein öffentlicher Zertifizierungsschlüssel (g^u) mit der ersten Zufallszahl (t) potenziert wird,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der ersten Nachricht (M1) aus der Identitätsgröße (|MU|) der Benutzercomputereinheit (U) ein zweiter verschlüsselter Term (VT2) gebildet wird, indem die Identitätsgröße (|MU|) mit dem Zwischenschlüssel

(L) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die erste Nachricht (M1) anstatt der Identitätsgröße (|MU|) der Benutzercomputereinheit (U) den zweiten verschlüsselten Term (VT2) aufweist,

— bei dem die vierte Nachricht (M4) anstatt der Identitätsgröße (|MU|) der Benutzercomputereinheit (U) den zweiten verschlüsselten Term (VT2) aufweist, und

— bei dem in der Zertifizierungscomputereinheit (CA), nachdem die vierte Nachricht (M4) empfangen wurde, der zweite verschlüsselte Term (VT2) entschlüsselt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4,

— bei dem die zweite Nachricht (M2) zusätzlich ein optionales erstes Datenfeld (dat1) aufweist, und

— bei dem die dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße zusätzlich mindestens das optionale erste Datenfeld (dat1) aufweist.

6. Verfahren nach einem der Ansprüche 1 bis 5,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der dritten Nachricht (M3) ein dritter verschlüsselter Term (VT3) gebildet wird, indem ein optionales zweites Datenfeld (dat2) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die dritte Nachricht (M3) zusätzlich mindestens den dritten verschlüsselten Term (VT3) aufweist, und

— bei dem in der Netzcomputereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde, der dritte verschlüsselte Term (VT3) entschlüsselt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der dritten Nachricht (M3) ein erster verschlüsselter Term (VT1) gebildet wird, indem der Signaturterm mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die dritte Nachricht (M3) anstatt des Signaturterms den ersten verschlüsselten Term (VT1) aufweist, und

— bei dem in der Netzcomputereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde und bevor der Signaturterm verifiziert wird, der erste verschlüsselte Term (VT1) entschlüsselt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem in der Netzcomputereinheit (N) die Antwort (A) gebildet wird, indem eine Konstante (const), die in der Netzcomputereinheit (N) und in der Benutzercomputereinheit (U) bekannt sind, mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird.

9. Verfahren nach einem der Ansprüche 1 bis 7,

— bei dem in der Netzcomputereinheit (N) die Antwort (A) gebildet wird, indem auf den Sitzungsschlüssel (K) eine dritte Hash-Funktion (h3) angewendet wird, und

— bei dem in der Benutzercomputereinheit (U) die Antwort (A) überprüft wird, indem auf den Sitzungsschlüssel (K) die dritte Hash-Funktion (h3) angewendet wird und das Ergebnis mit der Antwort (A) verglichen wird.

10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem in der Benutzercomputereinheit (U) die Antwort (A) überprüft wird, indem die Konstante (const) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird und das Ergebnis mit der Antwort (A) verglichen wird.

11. Verfahren nach einem der Ansprüche 1 bis 8, bei dem in der Benutzercomputereinheit (U) die Antwort (A) überprüft wird, indem die Antwort (A) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) entschlüsselt wird und eine entschlüsselte Konstante (const') mit der Konstante (const) verglichen wird.

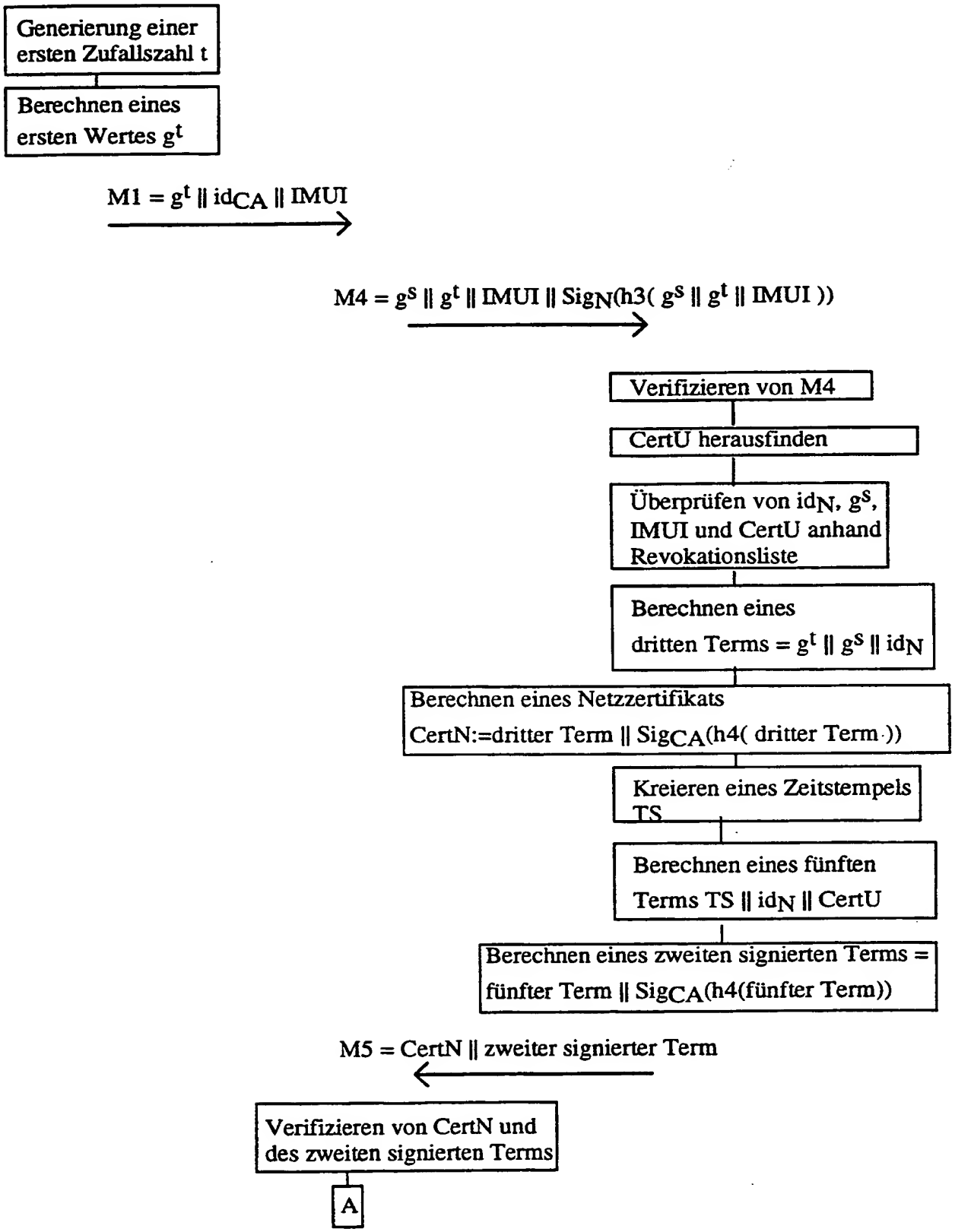
12. Verfahren nach einem der Ansprüche 1 bis 11, bei dem in der Zertifizierungscomputereinheit (CA) mindestens eine der Größen, die Identitätsangabe (id_N) der Netzcomputereinheit (N), die Identitätsgröße (|MU|) der Benutzercomputereinheit (U), der öffentliche Netzschlüssel (g^s) oder das Benutzerzertifikat (CertU) anhand einer Revokationsliste überprüft wird.

13. Verfahren nach einem der Ansprüche 1 bis 5, bei dem die dritte Nachricht (M3) zusätzlich mindestens ein optionales zweites Datenfeld (dat2) aufweist.

Hierzu 4 Seite(n) Zeichnungen

Nummer: DE 195 18 544 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 1. August 1996

Benutzercomputereinheit U Netz computereinheit N Zertifizierungscomputereinheit CA

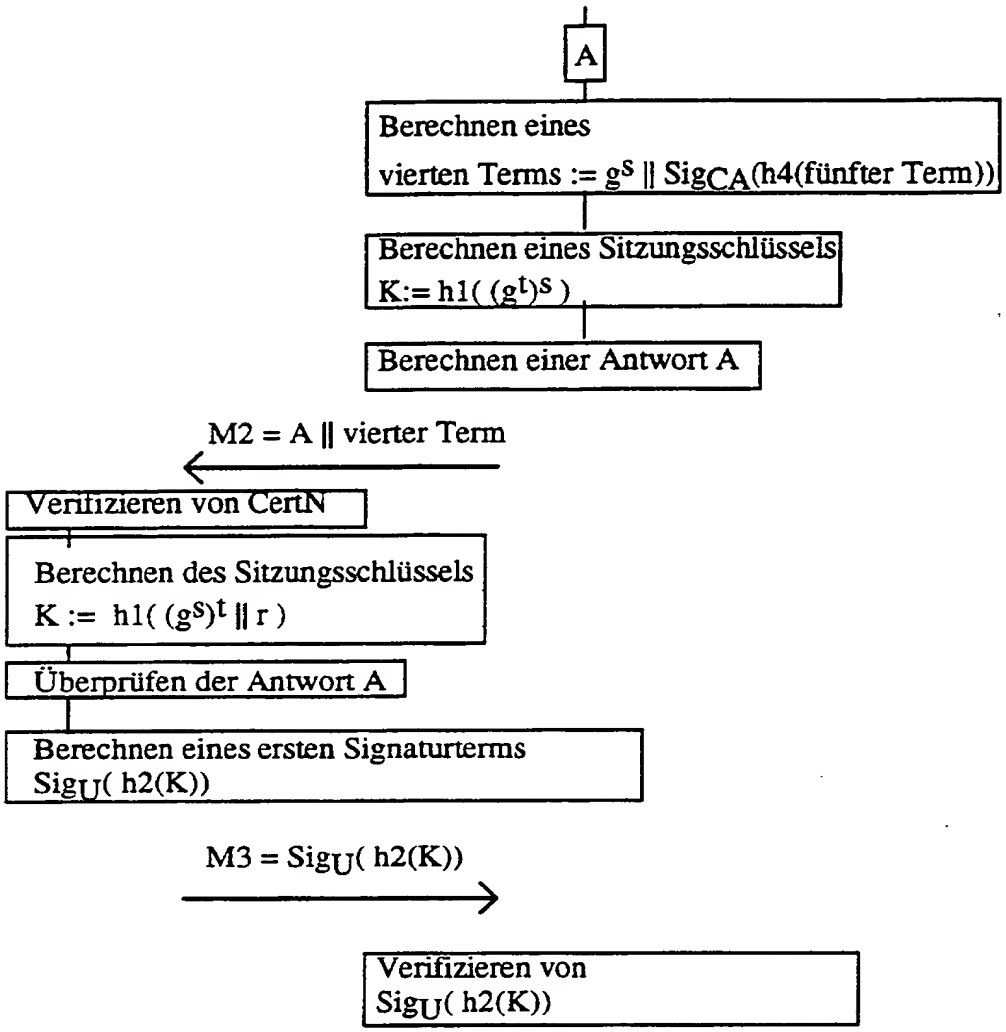


Figur 1a

602 131/258

Nummer: DE 195 18 544 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 1. August 1996

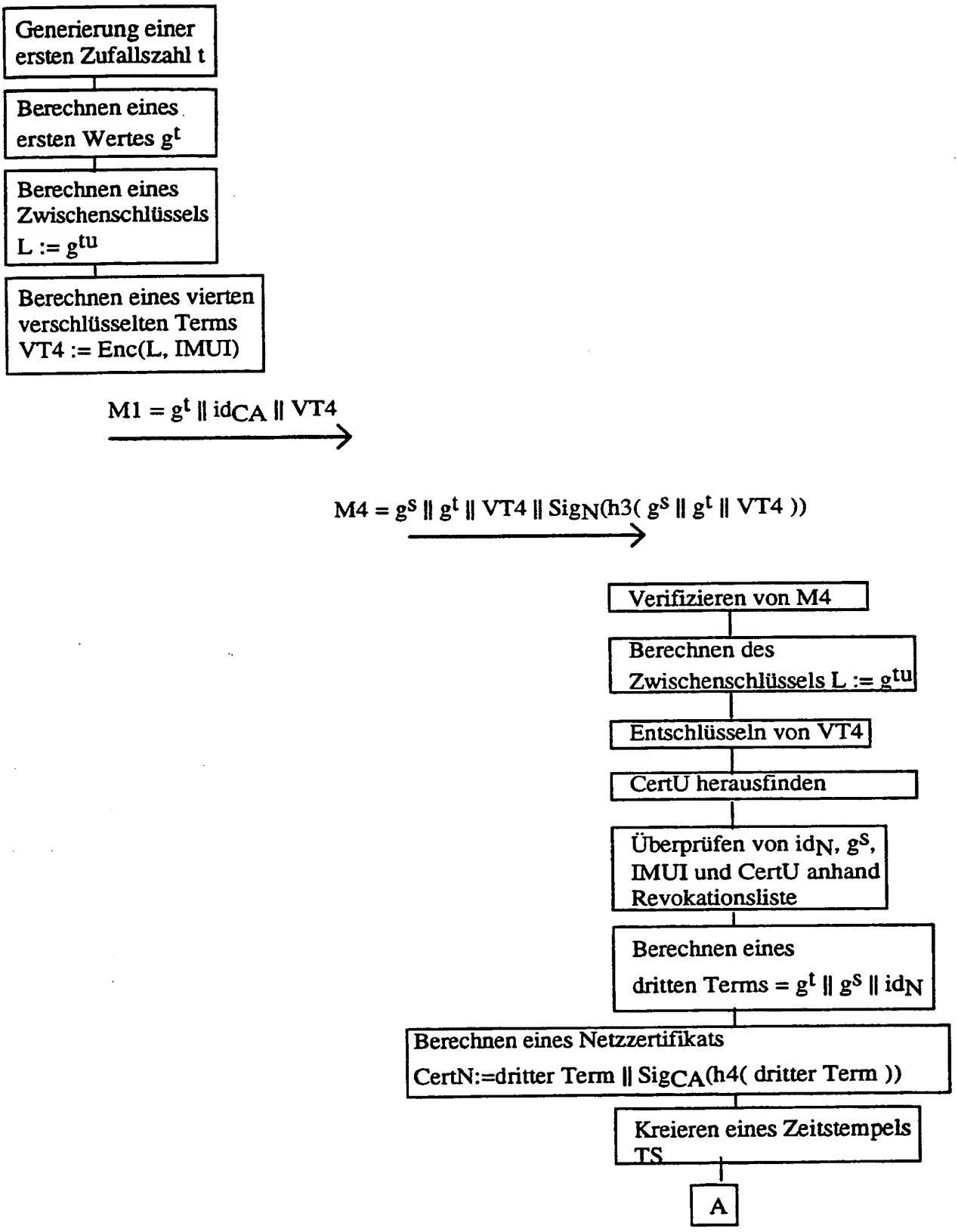
Benutzercomputereinheit U Netz computereinheit N Zertifizierungscomputereinheit CA



Figur 1b

Nummer: DE 195 18 544 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 1. August 1996

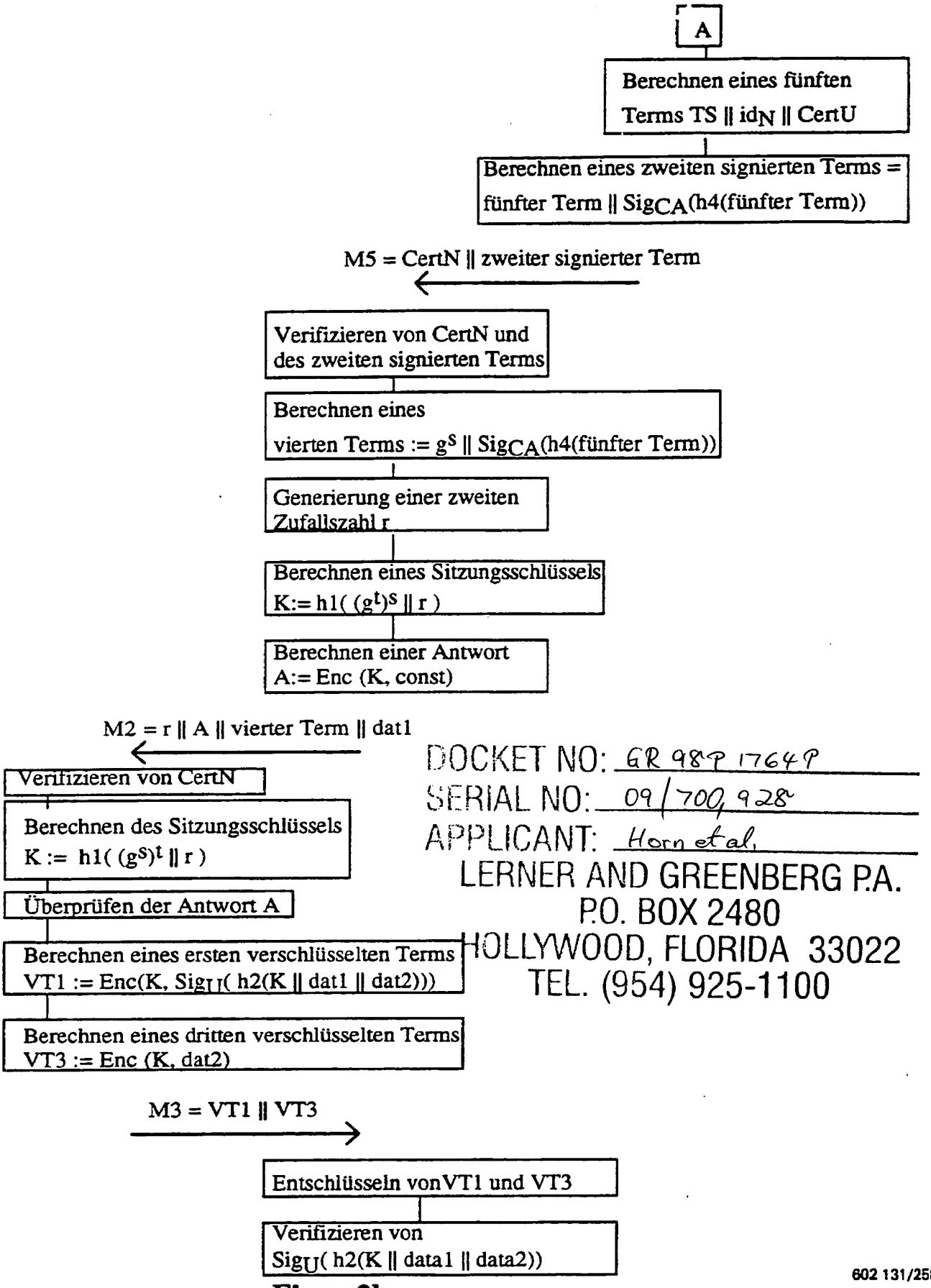
Benutzercomputereinheit U Netz computereinheit N Zertifizierungscomputereinheit CA



Figur 2a

602 131/258

Nummer: DE 195 18 544 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 1. August 1996



DOCKET NO: GR 98 P 1764 P
SERIAL NO: 09/709,928
APPLICANT: Horn et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100

602 131/258

Figur 2b